
Mid-Term Security Architecture

**Jan Filsinger
Chuck Pfleeger
H.O. Lubbes**

17 July 1996

AGENDA

- **Security Architecture Assumptions & Constraints**
- **Security Architecture**
- **Guard Functionality**
- **Guard Survey**
- **Next Steps**

Security Architecture Assumptions

- **Security within a federate and among its private data sources must be addressed by the individual federate.**
- **The RTI handles all data exchanged among and used by more than one federate.**
- **Sanitization rules are documented as part of the federation development process**
- **Classified information transmitted outside a protected security domain is encrypted**
- **Modeling and Simulation Resource Repository (MSRR) is not part of the run time HLA**

Security Architecture Assumptions

- **Need-to-know, release restrictions, handling caveats and the creation/deletion of special communities of interest are not addressed**
- **Integrity of data in transit will be assured by the RTI and communication mechanisms**

Security Architecture Constraints

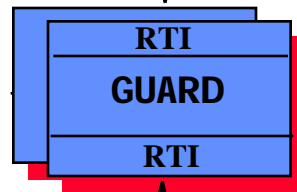
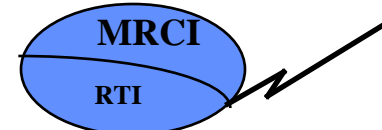
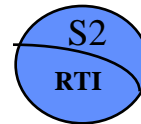
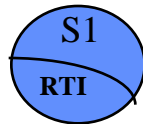
- **Source/destination identifiers are not sensitive**
 - a federate that subscribes to a data item is willing to receive data from any federate willing to publish it
 - a federate may be able to infer the source of a data item but knowledge of that source is not security-relevant
- **Two-way guard is required to support information flow in both directions**
- **The guard and the RTI segments reside on a trusted platform**
- **All communications crossing security domains will go through a guard**
- **The architecture supports multiple security domains (there will be a practical limit that can be supported)**

Security Architecture - Mid Term

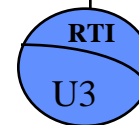
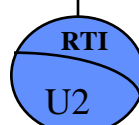
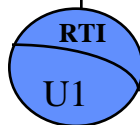
- **An RTI is instantiated with the security level used within the domain**
- **The guards mediate the transfer data and control services between security domains**
 - *All* RTI services between domains pass through the guard
- **To the RTI, the guard will appear to be a Federate**
- **To a federate, the guard will appear to be the RTI**

Security Architecture -- Mid Term

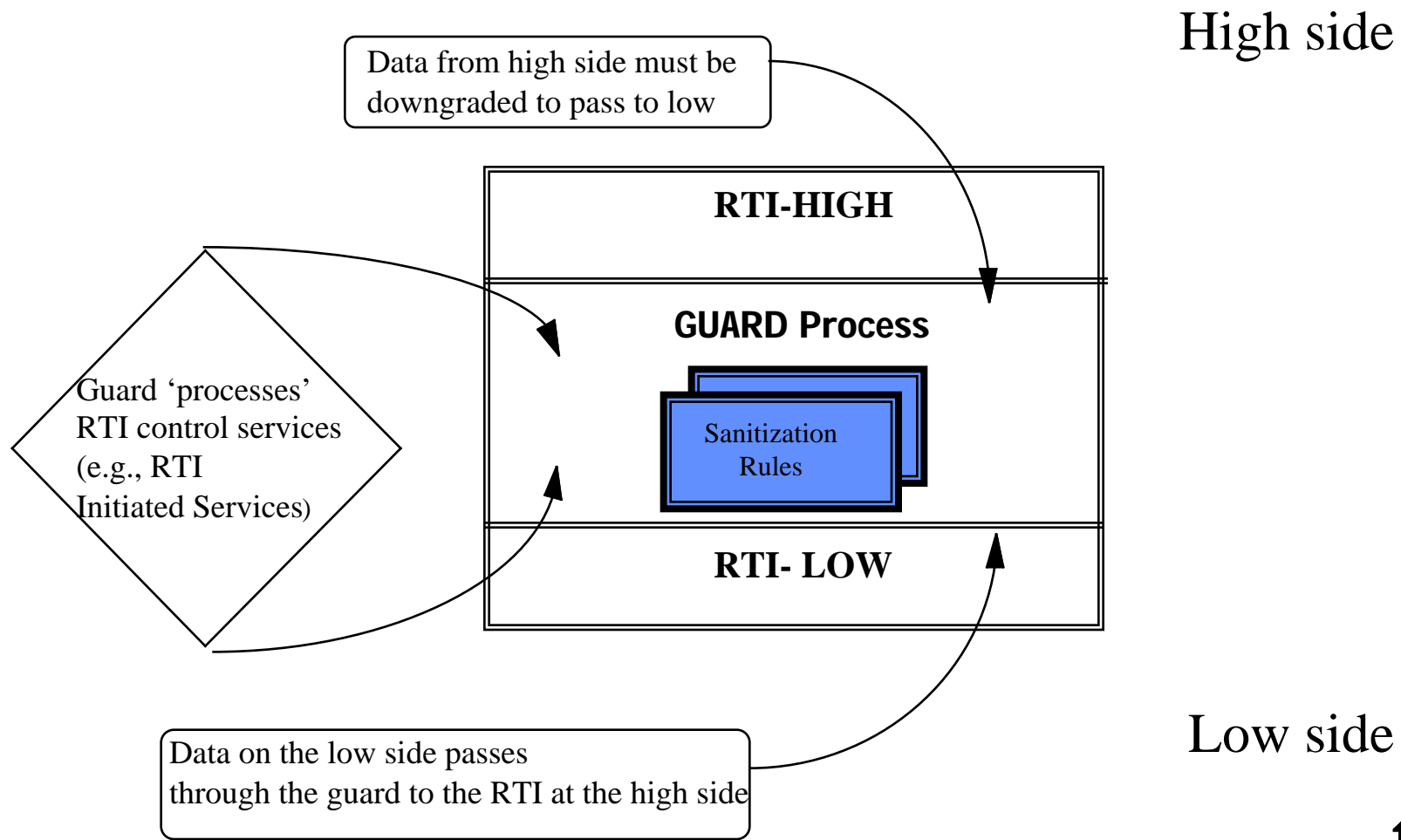
SECRET
Domain



UNCLASSIFIED
Domain



Guard Functionality



Guard Survey: Candidate Guards

- **Command and Control Guard (C2G)**
- **Radiant Mercury**
- **Generic Trusted Intermediary (GTI)**

- **Formerly WWMCCS Guard**
- **Supports fully automated high-to-low and low-to-high transfers**
- **High assurance design; supported on high assurance platform (Wang/Honeywell XTS-300)**
- **Operational in U.S. Forces Korea**

Radiant Mercury

- **Designed for fully automatic high-to-low sanitization**
- **Message-oriented**
- **Based on Hewlett-Packard B1 HPBLS Unix platform**
- **Table-driven, reconfigurable sanitization; imagery sanitization under development**
- **Operational and accredited at several sites**



- **IR&D Effort of SAIC**
- **Operational at DARPA as Distributed Interactive Simulation (DIS) Guard**
- **Supports Secret to Unclassified information flow**
- **Based on Sun B1 CMW.**
- **Designed for ease of reconfiguration of security policy/sanitization rules**
- **System modular; modules reconfigurable for specific requirements**

Guard Survey: Results

- **Unlikely that COTS or GOTS guard will currently fit all HLA requirements**
- **Several promising GOTS products provide needed functionality, with high assurance, at reasonable cost**
- **Sample sanitization/releasability rules needed for more complete exploration of guard capabilities**